



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/041,964	01/09/2002	Makoto Oka	SON-2320	4260

7590 02/07/2007  
RADER, FISHMAN & GRAUER, P.L.L.C.  
Suite 501  
1233 20th Street, NW  
Washington, DC 20036

EXAMINER
----------

POWERS, WILLIAM S

ART UNIT	PAPER NUMBER
----------	--------------

2134

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/07/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/041,964	<b>Applicant(s)</b> OKA ET AL.	
	<b>Examiner</b> William S. Powers	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 21 November 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.


#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 January 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
KAMBIZ ZAND  
PRIMARY EXAMINER

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments filed 11/21/2007 have been fully considered but they are not persuasive.

As to Applicant's argument that Vaeth "does not generally describe the sequence of having the registration authority receive a public key certificate issuance request and transmitting the same to the same to the certificate authority" (Remarks, page 13), Applicant is directed to column 7, lines 59-65 of the Vaeth patent wherein the requestor clearly accesses a web page maintained by the RA to request a certificate and that request is forwarded to the CA.

As to Applicant's argument that "the certificate authority does not have a plurality of signature modules each executing a different encryption algorithm" (Remarks, page 13), Applicant is directed to column 6, lines 32-43 of the Vaeth patent. Crypto cards are responsible for generating private keys used by the CA to sign and encrypt certificates and messages. The CA has a plurality of private keys, supplied by multiple crypto cards that are used to sign and encrypt certificates issued by the CA.

As to Applicant's argument that the Vaeth does not teach, "identifying the encryption algorithm that should be used based upon a table that associates the requesting RA to the encryption algorithm", Applicant is directed to column 8, lines 35-48 of the Vaeth patent. The RA verifies CRD data from the user with the registration database. If the verification is successful, the RA approves the certificate request and forwards it to the CA. As noted before, the private keys used by the CA to sign and encrypt messages and certificates are generated and stored in the crypto cards of the requestors. Therefore, when the RA approves and forwards a certificate request to the CA, the RA is associated with the requestor, the crypto card and the private keys used in signing and encryption operations.

### ***Response to Amendment***

In light of Applicant's amendment, the previous 35 USC 112, 2<sup>nd</sup> paragraph rejections of claims 2, 13, 16, 17, 22, 24 and 35 are withdrawn.

### ***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32 and 34-36 are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth).

As to claims 1, 14, 23 and 36 Vaeth teaches:

- a. A certificate authority for issuing a public key certificate used by an entity (column 8, lines 35-48).
- b. A registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority (column 8, lines 35-48).
- c. Wherein said certificate authority, having a plurality of signature modules (crypto cards) each executing a different encryption algorithm (column 7, lines 41-47), selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with an the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate (Different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is

forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate.) (column 7, lines 41-47 and column 8, line 35-column 9, line 12).

As to claims 2 and 24, Vaeth teaches:

- a. Said certificate authority has a certificate authority server for outputting a signature processing request to said plurality of signature modules (column 9, lines 24-31).
- b. Wherein said certificate authority server receives said public key certificate issuance request from said registration authority, selects at least one of said plurality of signature modules in response to said public key certificate issuance request, and outputs said signature processing request to the selected signature module (column 9, lines 24-45).
- c. Wherein each selected signature module attaches a digital signature to the message data constituting said public key certificate in response to said signature processing request received from said certificate authority server (column 7, lines 41-47).

As to claims 3 and 25, Vaeth teaches:

- a. Said certificate authority has a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with an

encryption algorithm specific to each of said registration authorities (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities and these associations are determined through screening functions performed by the CA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

b. Wherein, given a public key certificate issuance request from any registration authority, said certificate authority selects the signature module associated with the relevant encryption algorithm based on said registration authority management data (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities and these associations are determined through screening functions performed by the CA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

As to claims 5 and 27, Vaeth teaches said registration authority management data include signature module identification information applicable to signatures (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, these associations are determined through screening functions performed by the CA and thereby the proper signature is applied to the certificate as dictated by the associated RA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

As to claims 6 and 28, Vaeth teaches:

- a. Said registration authority transmits encryption algorithm designation information along with said public key certificate issuance request to said certificate authority (the algorithm designation information is the RA itself and the associations are determined through screening functions performed by the CA and thereby the proper signature is applied to the certificate as dictated by the associated RA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).
- b. Wherein said certificate authority, based on said encryption algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated encryption algorithm (Different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate.) (column 7, lines 41-47 and column 8, line 35-column 9, line 12).

As to claims 9, 19 and 31, Vaeth teaches said certificate authority uses at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate (joint approval scheme) (column 8, lines 49-59).



As to claims 10, 20 and 32, Vaeth teaches said certificate authority selects at least two of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation (joint approval scheme) (column 8, lines 49-59).

As to claims 12 and 34, Vaeth teaches at least part of said plurality of signature module have a common signature key stored therein (storage of the CA's private keys) (column 6, lines 32-39).

As to claims 13, 22 and 35, as best understood by the Examiner, Vaeth teaches each of said selected signature modules is configured to execute multiple encryption algorithms (column 8, lines 49-59).

As to claim 15, Vaeth teaches:

- a. Causing a certificate authority server to receive a public key certificate issuance request from said registration authority (column 9, lines 24-31).
- b. Causing said certificate authority server to select at least one of said plurality of signature modules in response to said public key certificate issuance request (column 9, lines 24-45).
- c. Causing said certificate authority server to output a signature processing request to the selected signature module (column 7, lines 41-47).

Art Unit: 2134

As to claim 16, Vaeth teaches said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with an encryption algorithm specific to each of said registration authorities (Different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate.) (column 7, lines 41-47 and column 8, line 35-column 9, line 12).

As to claim 17, Vaeth teaches said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on encryption algorithm designation information received along with said public key certificate issuance request (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities and these associations are determined through screening functions performed by the CA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claim 4 and claim 7 and claim 26 and claim 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth) as applied to claim 1 and claim 6 and claim 25 and claim 28 above respectively in view of US Patent No. 6,202,157 to Brownlie et al. (hereinafter Brownlie).

As to claims 4 and 26, Vaeth does not expressly mention storing the key length and parameter data of the signatures in a database. However, in an analogous art, Brownlie teaches management data that includes key length and parameter information applicable to signatures (Brownlie, column 3, lines 25-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certificate system of Vaeth with the storing of parameter information of the signature algorithms of Brownlie in order to "allow enforcement of the policies to occur at the network nodes to help reduce overhead requirements of a central authority," as suggested by Brownlie (Brownlie, column 2, lines 31-33).

As to claims 7 and 29, Vaeth as modified teaches said encryption algorithm designation information includes key length and parameter information applicable to signatures (Brownlie, column 3, lines 25-49).

7. Claim 8 and claim 18 and claim 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth) as applied to

claim 1 and claim 14 and claim 23 respectively above, and further in view of "On the Importance of Checking Cryptographic Protocols for Faults," by Boneh et al. (hereinafter Boneh).

As to claims 8, 18 and 30, Vaeth teaches:

- a. Said certificate authority has a verification key database which stores signature keys of the crypto cards and certificates (crypto cards (column 6, lines 32-38) and RAID array to store CRDs and certificates (column 10, lines 34-36)).

Vaeth does not expressly mention the verifying of the certificate authority signatures by the certificate authority. However, in an analogous art, Boneh teaches said certificate authority verifies signatures generated by each of said plurality of signature modules (Boneh, page 38, lines 28-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certificate system of Vaeth with the signature verification of Boneh in order to maintain the security of the certificate authority and prevent the generation of fake certificates as suggested by Boneh (Boneh, page 37, lines 11-17).

8. Claim 11 and claim 21 and claim 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth) as applied to claim 1 and claim 14 and claim 23 respectively above, and further in view of US Patent No. 6,675,296 to Boeyen et al. (hereinafter Boeyen).

As to claims 11, 21 and 33, Vaeth teaches that registration authorities are associated with respective crypto cards (signature modules) and the appropriate signature is attached to the certificate (column 8, lines 35-59), but does not expressly mention the use of identifiers. However, in an analogous art, Boeyen teaches certificate generator that has a digital format selector (identifier) that is used in selecting the proper signature from the certificate template data (Boeyen, column 6, line 62-column 7, line 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certificate system of Vaeth with the signature selector of Boeyen in order to ensure that the proper signature type is attached to a certificate.

### ***Conclusion***

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the

Art Unit: 2134

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zand Kambiz can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



William S. Powers  
Examiner  
Art Unit 2134



KAMBIZ ZAND  
PRIMARY EXAMINER

Application/Control Number: 10/041,964  
Art Unit: 2134

Page 15

2/2/2007